REMARKS

In response to the Official Action dated 10/1/2007, the above-identified application has been amended to place the claims in better condition for allowance. Review and reconsideration are requested in view of the above amendments and following remarks.

The drawings were objected to as not showing all claimed features. A replacement drawing is submitted herewith. Withdrawal of the objection is kindly requested.

The Office Action indicated that the claims and specification did not provide support for the claimed language as previously submitted.

Specifically, it is stated

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification fails to provide proper antecedent basis for the recitations of *"a first SSL connection between said client and said web server"*, *"a second SSL connection between said client and said server in a manner which permits optimization techniques to be performed on data transmitted through said second SSL connection"*, *"means for permitting establishing a first SSL connection...and permitting a*

second SSL connection", and *"means for establishing said first SSL connection and... for enabling said second SSL connection between said client and said server in a manner which permits optimization techniques to be performed on data transmitted through said second SSL connection".*

Claims 1-19 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement for the reasons recited above.

Applicants kindly traverse. First, it is noted that the phrase "performed on data" in the claims has been replaced with "applied on data". In this regard, the phrase "means for permitting establishing" is changed to "means for enabling". These amendments are submitted to be a change in words to accommodate the examiner's position by providing the identical terms used in the specification as opposed to similar words conveying similar meaning and are not a type of change which would trigger a change in scope of claim interpretation.

Set forth are the pertinent parts of the originally filed specification which are italicized in part to demonstrate the claimed language is clearly supported as well as the amended language to the specification submitted herewith. Comments are in bold and bracketed.

At page 6, lines 2-22, page 7, lines 1-22 and page 8, lines 1-2 of the filed Specification, the following is stated:

> The present invention is generally depicted in FIGS. 2A and 2B and is directed to a system and method for increasing data access in a secure socket layer network environment and is generally designated by the number 100. The system 100 includes a *web server computer 102* which has an operating system/software, server software, memory and linking devices as is known in the art. Further, the *computer 102 has SSL protocol server software operably disposed thereon for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key.*
>
> A *client computer 104* includes an operating system/software, web browser software having SSL protocol client software operably disposed *thereon for enabling a*

SSL connection, memory and linking devices as is known in the art and is communicatively linked to the web server computer 102. SSL acceleration client (SSLAC) software is operably disposed on the client computer 104 for monitoring when the web browser requests a SSL connection with the web server 102.

SSL acceleration server (SSLAS) software is operably disposed on the web server computer 104 for receiving a request for a SSL connection through SSL acceleration client software. The SSL acceleration server software is operably associated with the SSL protocol server software to obtain one either a copy or an equal credential of the CA certificate (i.e., a pseudo CA certificate) and private key.

The operation of the invention can be understood from steps shown in FIGS. 2A and 2B. *SSL acceleration client software intercepts 200 new SSL request for a SSL secure connection from the web browser to a target web server. The SSL acceleration client software then initiates 202 a SSL handshake with the SSLAS operably associated with the target web server computer and to start SSL connection.* The SSLAS then determines 204 which CA certificate is operably associated with the target web server. As part of the SSL handshake between SSLAC and SSLAS, the SSLAS sends 206 this CA certificate to SSLAC along with a public key. *At this point a secure SSL session is established between SSLAC and SSLAS and all subsequent data traffic between SSLAC and SSLAS flows over this secure connection.* **[i.e., a first SSL connection]** *The SSLAC software sends 208 the copy of the CA certificate to the web browser for validation 210. Web browser software sends 212 a list of available encryption algorithms (ciphers) back to target web server (i.e., server computer 102). SSLAC software intercepts this from the browser and sends 214 a chosen cipher to the browser software. The web browser software creates 216 a secret key, encrypts using chosen cipher and using the previously received public key and sends 218 the encrypted secret key to the target server, which is intercepted and sent 219 through the SSL acceleration client software to the SSLAS software. SSLAS software de-encrypts 220 the secret key using the private key operably associated with the target server. SSLAS software sends 222 decrypted secret key back to SSLAS software via the secure SSL connection, wherein a "handshake" is completed and secure communications between the client computer's web browser and SSLAS softwar e* **[i.e., a first SSL connection]** *and by using the secret key, data can be accelerated between the client computer 104 and the web server computer 102 employing acceleration software, such as compression software of the SSL acceleration client/server software.*

Because the SSL connection is terminated by SSLAC, *SSLAC can process the data in unencrypted form allowing it to apply data compression and other optimization techniques to the data stream.* This is done in such a way that the credentials of the SSLAS are presented to the web browser without having violated the SSL paradigm because the private key of the SSLAS was never transmitted to SSLAC.

The specification clearly discloses a client computer, web server, first and second SSL connections wherein the second permits optimization techniques to be applied on the data

transmitted through the second SSL connection. There is also clearly disclosed the means for enabling each connection. Accordingly, withdrawal of the rejection to the specification and claims is kindly requested.

In the Office Action of 10/1/2007, the Examiner states as follows:

Claims 1 – 8 and 10 – 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al. (Aziz), "Method and Apparatus for Providing Secure Communication with a Relay in a Network", U.S. Patent 6,643,701 in view of Gast, "System and Method for Accelerating Cryptographically Secured Transactions", U.S. Patent Publication 2003/0046532.

Applicants kindly traverse. Aziz does not alone or in combination with any of the cited references teach, disclose or suggest the claimed invention. Aziz is directed to a method and apparatus for providing secure communication with a relay in a network. Converse to the examiner's position, Aziz teaches away from the present invention. Col. 6, lines34-48 state"

> In FIG. 3, a server 340 provides intermediate relays 320 with information that can authenticate the relays as server 340. Each client 300 negotiates an end-to-end secure transmission link 310 with a particular relay 320. Each relay is connected to a server through another end-to-end secure transmission link 330 to server 340. This structure allows secure transmission of information from the client 300 to server 340.
>
> If the network between relays 320 and server 340 is trusted (as would be the case if the relays, network, and server were all in the same facility) and therefore secure, connection 330 could even be cleartext HTTP connection, reducing the server workload even more compared to using previously negotiated SSL sessions, as will be discussed below.

It is clear that Aziz only discloses making a single connection between each client and a

relay and a relay and a server. Moreover, Aziz states that the connection can be a cleartext HTTP connection. This can be a problem and create a security issue because Basic credentials are Base64-encoded. If Basic credentials are sent over an HTTP connection, they may be read as clear text and decoded.

Column 6, lines 4-24 simply indicate that there could be multiple clients, relays or servers. However, in the cases disclosed each paradigm fails to show multiple SSL connections between the same client and server. Rather, there is simply shown the inclusion of the means to create a single secure connection between the client/relay and relay/server.

There is no disclosure, suggestion or teaching in Aziz as to the need or means how to make multiple SSL connections with the same client and same server. This is only taught by the present invention.

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [paragraph 0015]. Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional SSL connection between the client and server as opposed to the instant invention which provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections through whereby data can pass in a compressed form, for example, in the second established connection. Gast teaches away from the instant invention.

Likewise as stated above, Aziz attempts leads toward offloading the SSL connection by

using a cleartext HTTP connection, i.e., Aziz states "reducing the server workload even more compared to using previously negotiated SSL sessions". Combining the references in no way would result in the present invention and in fairly interpreting the teachings of each and combining such teachings a reasonable combination at best would be the combination of offloading encryption processing further with the aid of relays. This does not render the instant invention. Withdrawal of the rejection of claims under 35 U.S.C. over Aziz in view of Gast is respectfully requested.

The Examiner stated:

> **Claims 9 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Aziz and Gast in view of Freed et al. (Freed), "Secure Sockets Layer Proxy Architecture", U.S. Patent Publication 2003/0014628.**

This is also traversed. Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration. Like Aziz, there is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. Nevertheless, the tertiary computer employs conventional handshake technology.

This is very different from the instant invention. The present invention calls for a system

for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second SSL connection. A method employing these elements is also provided.

The instant invention provides a server with SSL protocol server software and SSL acceleration server software on both the client and server for enabling direct and multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created. Freed et al., like Aziz, introduces a third element in the chain of connection and another potential break point for communication.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. (or Aziz) and this can't be accomplished in the teachings of Freed et al or Aziz. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

It is respectfully submitted that the instant claimed invention is not taught, disclosed or suggested by Aziz, Gast or Freed et al. taken alone or together. The instant invention is respectfully submitted to be patentably distinct over the art of record. Withdrawal of the rejection of claims 1-19 is respectfully requested.

Therefore, allowance of claims 1-19 is requested at as early a date as possible. This is intended to be complete response to the Official Action dated 10/1/2007 which fell due on a holiday.

Respectfully submitted,

/R. William Graham/

R. William Graham, 33,891

Certificate of Transmission

I hereby certify that this correspondence is being electronically filed with the PTO for group 2137on the date shown below.

/R. William Graham/

Date. Wednesday, January 02, 2008 R. William Graham, 33,891